第6章 局域网与网站安全

前面的章节介绍了计算机网络的威胁与表现形式，以及计算机网络模型中的安全协议及安全体系。由于防火墙以及各种隔离、防御技术的发展，从外部网络直接入侵内部网络已经越发困难。很多黑客已经转变了思路，从内部局域网入手，反向进行渗透，达到入侵的目的。本章将向读者介绍局域网的常见威胁手段及防御措施、网站的安全防护以及入侵检测系统的应用。

重点难点

- 局域网简介
- 局域网常见的攻击方式与防范
- 无线局域网的安全技术
- 无线密码的破解及防御
- 网站的抗压检测
- 入侵检测技术应用

6.1 局域网的安全威胁

局域网是现在应用范围最广的网络类型，日常接触到的网络中，绝大多数都是局域网。所以保障局域网的安全性尤为重要。下面介绍局域网以及局域网常见的安全威胁及防范。

6.1.1 局域网简介

局域网（Local Area Network，LAN）指在小范围内，一般不超过10km，将各种计算机终端及网络终端设备，通过有线或者无线的传输介质组合成的网络，用来实现文件共享、远程控制、打印共享、电子邮件服务等功能。局域网相对来说私有性较强。因为范围较小，所以传输速度更快，性能也更稳定，组建成本相对较低，技术难度不高。完整的家庭或小型公司的无线局域网的拓扑图如图6-1所示，大中型企业的局域网相对要更复杂一点。

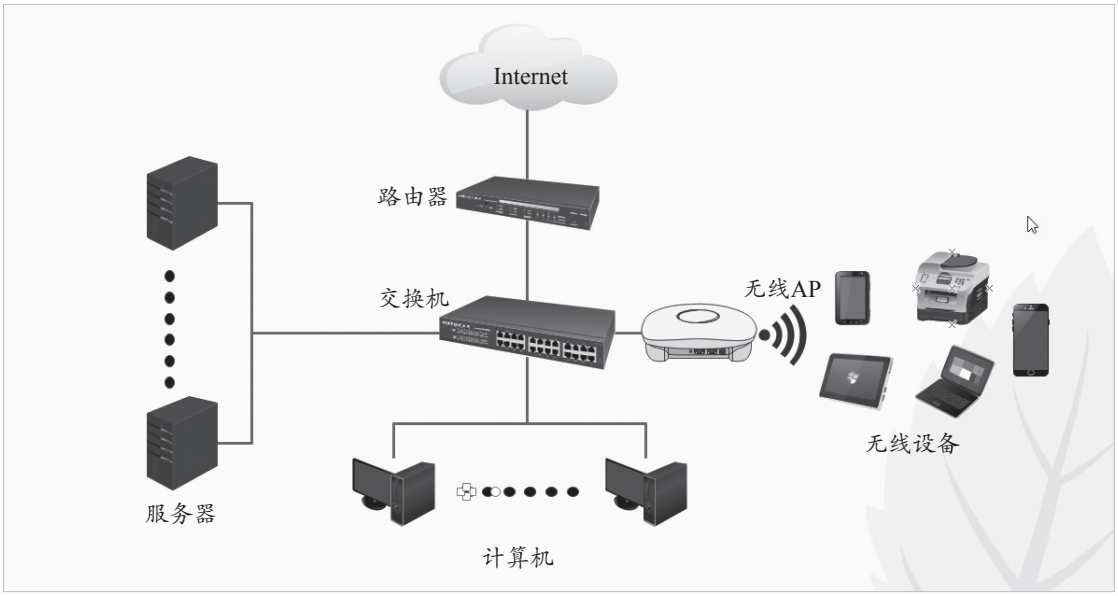


图 6-1

知识点拨

局域网常见的结构

局域网通常分为总线型、星形、环状、树形等拓扑结构。

6.1.2 常见安全威胁及防范

局域网常见的安全威胁就是各种欺骗技术了，黑客会将自己的设备伪装成局域网的关键设备，如网关服务器、DNS服务器、DHCP服务器等，通过这种方式获取用户的数据包，然后进行篡改或破译，从而获取用户数据，或者直接进入数据库主机中下载数据，并上传给黑客。

1. ARP 欺骗和防范

ARP（Address Resolution Protocol）地址解析协议，作用是将IP地址解析成MAC地址。只有知道了IP地址和MAC地址，局域网中的设备才能互相通信。ARP攻击最典型的例子，就是伪

装成网关。黑客的主机监听局域网中其他设备对网关的ARP请求（设备想要知道网关的MAC地址，以便封装数据包），然后将自己的MAC地址回应给请求的设备。这些设备发给网关的数据，全部发给了黑客的主机。黑客就可以收集并通过多种方法破译数据包中的信息或篡改数据。正常情况下，黑客并不阻拦数据包，而是将自己的设备伪装成受害设备，将包继续发给网关，这样从受害者和网关的角度，都不会发现异常。ARP攻击的示意图如图6-2所示。

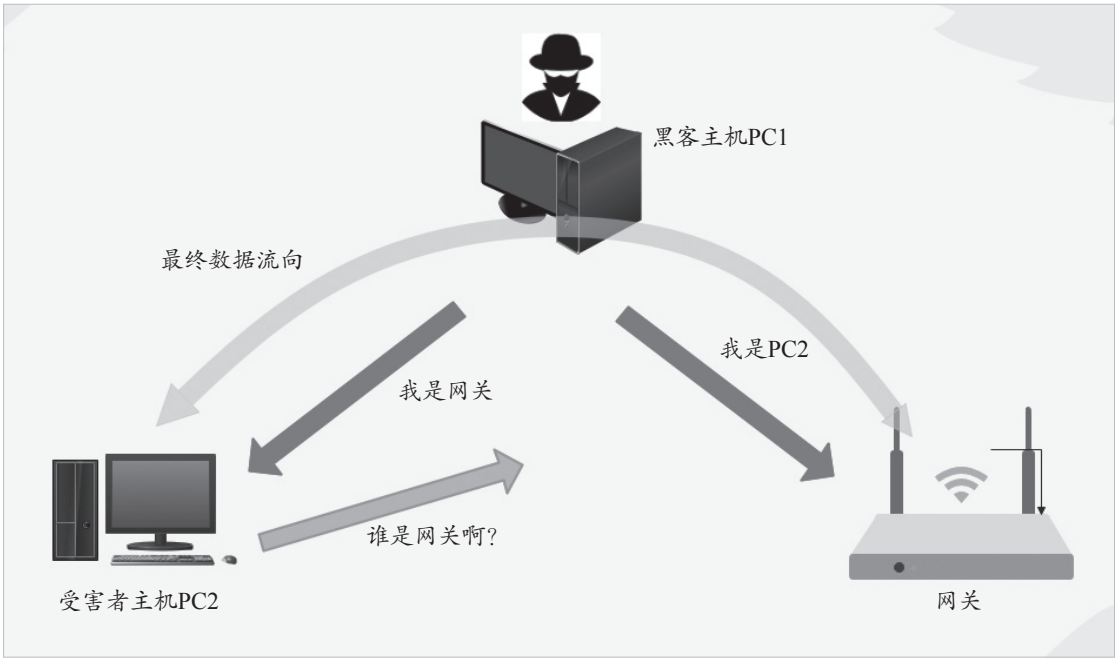


图 6-2

ARP攻击除了可以获取数据包外，还可以让受害者断网、控制对方的网速等。其实ARP欺骗起初也可以作为一种网络管理手段。而要防范ARP欺骗，可以安装ARP防火墙，或者将IP地址和MAC地址绑定（在设备及网关上都要绑定），这样就不需要ARP解析，也就不会发生ARP欺骗了。绑定的缺点是该IP不能随意更换，否则会造成网络不通。

知识点拨

DHCP欺骗

DHCP（Dynamic Host Configuration Protocol，动态主机配置协议）用来使主机自动获取IP地址等网络参数。与ARP欺骗类似，DHCP欺骗也通过回应伪造的DHCP应答，并分配给受害主机IP地址等信息，将网关地址设置为自己的地址。这样受害主机的所有数据包都会被黑客截获。防范措施同样是使用防火墙，并进行IP地址和MAC地址的绑定。

2. DNS 欺骗和防范

DNS（Domain Name System，域名系统）欺骗也叫作DNS劫持。DNS是用来将网站域名（www.×××.com）解析成IP地址（a.b.c.d）的。只有经过解析，客户端才能访问。DNS欺骗是黑客将自己的计算机伪装成提供这种服务的设备，给用户提供虚假解析。比如用户访问某域名www.×××.com，经过正常的DNS解析，应该是a.b.c.d，而黑客可以更改成e.f.g.h，从受害者的角度来说，域名绝对没有输错，而返回的e.f.g.h是黑客伪造的一模一样的钓鱼网站，后果就可想

而知了。用户的用户名、密码、手机号等全部会被黑客获取。DNS欺骗原理如图6-3所示。解决方法是手动设置正常的DNS地址即可。

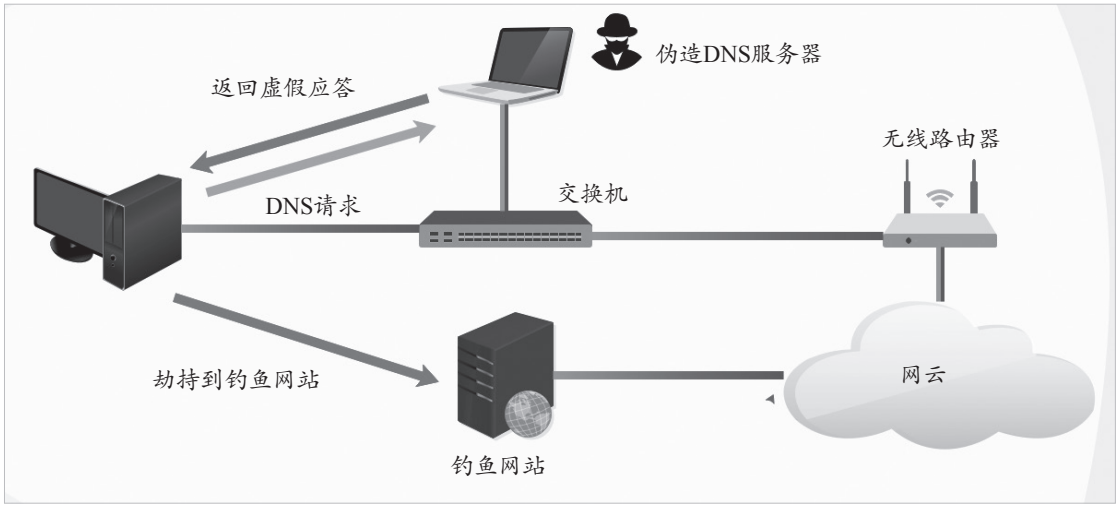


图 6-3

3. 生成树欺骗与防范

生成树是网络设备“交换机”的一种协议，用来防止网络设备环路的产生。通过该协议，网络产生备份和冗余。而黑客通过欺骗，修改协议参数，将自己伪装成网络中的一台交换机，这样所有的数据都会被黑客截获，如图6-4所示。

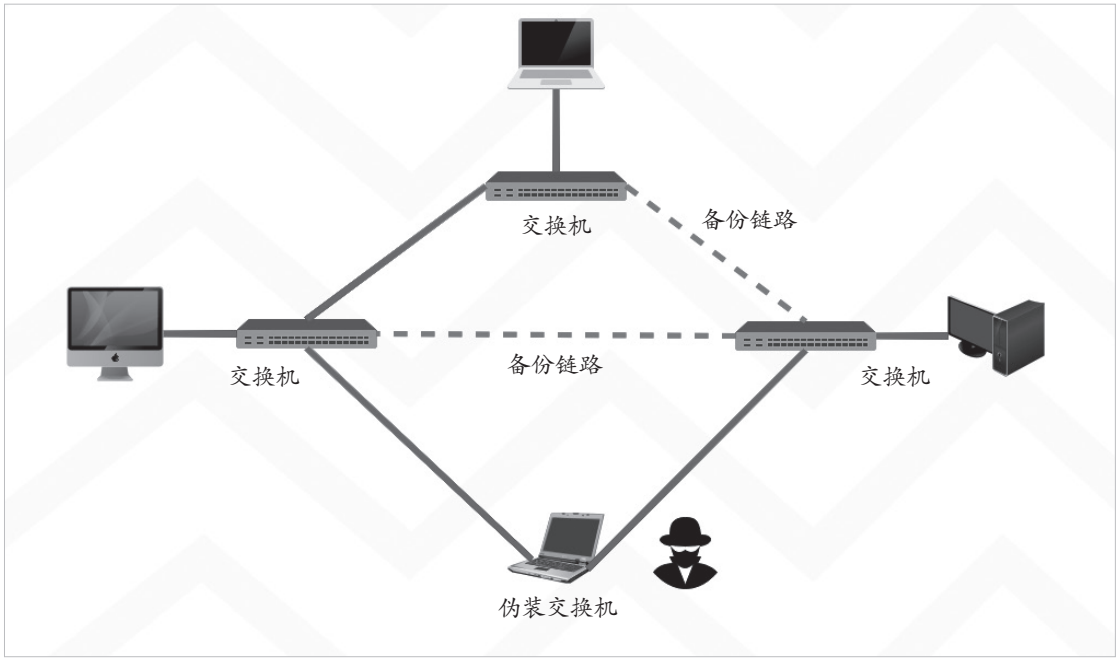


图 6-4

为避免生成树欺骗攻击，可将交换机用于主机接入的端口设为边缘端口，或者手动配置主用和备用根设备，启用根防护。

6.2 无线局域网的安全威胁

无线局域网是加入了无线技术的局域网，下面重点介绍无线技术中常见的安全威胁以及防范措施。

6.2.1 无线局域网及其技术

无线局域网（Wireless Local Area Network，WLAN）指应用无线通信技术将计算机设备互联起来，构成可以互相通信和实现资源共享的网络体系。无线局域网的本质特点是不再使用通信电缆将计算机与网络连接起来，而是通过无线的方式连接，从而使网络的构建和终端的移动更加灵活。

目前无线局域网已经遍及生活的各个角落：家庭、学校、办公楼、体育场、图书馆、公司、大型企业等都有无线技术的身影。另外无线技术还可以解决一些有线技术难以覆盖或者布置有线线路成本过高的地方，如山区、跨河流、湖泊以及一些危险区域。

无线局域网工作于2.5GHz或5GHz频段，是很便利的数据传输系统，它利用射频技术取代原有比较碍手的双绞线构成的局域有线网络。无线局域网是介于有线传输和移动数据通信网之间的一种技术，可提供用户高速的无线数据通信。目前的无线局域网产品所采用的技术标准主要有蓝牙、HomeRF、HiperLAN、IEEE 802.11等。

1. 蓝牙

蓝牙（Bluetooth）是一种短距离的、开放性无线通信标准，设计者的初衷是用隐形的连接线代替线缆，蓝牙的出现不是为了竞争而是互补。利用蓝牙技术能够有效地简化移动通信终端设备之间的通信，也能够成功地简化设备与Internet之间的通信，从而使数据传输变得更加迅速高效，为无线通信拓宽道路。蓝牙在发射带宽为1MHz时，其有效数据传输速率为721kb/s，最高数据传输速率可达1Mb/s。由于采用低功率时分复用方式发射，其有效传输距离约为10m，加上功率放大器时，传输距离可扩大到100m。蓝牙不仅采用了跳频扩谱的低功率传输，而且还使用鉴权和加密等方法提升通信的安全性。

2. HomeRF

HomeRF是专门为家庭用户设计的无线局域网技术标准，是IEEE 802.11与DECT的结合，旨在降低语音数据成本。HomeRF采用跳频扩频（Frequency Hopping Spread Spectrum，FHSS）方式，可以同时使用4个高质量的语音信道通信，可以使用时分复用（Time Division Multiplexing，TDM）进行语音通信，也可以通过CSMA/CA协议进行数据通信业务。

3. HiperLAN

HiperLAN 1推出时，数据传输速率较低，没有被人们重视，2000年，HiperLAN 2标准制定完成，HiperLAN 2标准的最高数据传输速率为54Mb/s，详细定义了无线局域网的检测功能和转换信令，用以支持更多无线网络，支持动态频率选择、无线信元转换、链路自适应、多束天线和功率控制等。该标准在无线局域网性能、安全性、服务质量QoS等方面也给出了一些定义。

4. IEEE 802.11

IEEE 802.11无线局域网标准的制订是无线网络技术发展的一个里程碑。802.11标准的颁布，使得无线局域网在各种有移动要求的环境中被广泛接受，它是目前无线局域网最常用的传输协议，各个公司都有基于该标准的无线网卡产品。

现在的无线局域网主要以802.11为标准，定义了物理层和MAC层规范，允许无线局域网及无线设备制造商建立互操作网络设备。基于IEEE 802.11系列的常见标准，其中，802.11a、802.11b、802.11g、802.11n、802.11ac和802.11ax最具代表性。各标准的有关数据如表6-1所示。

表 6-1

协议	使用频率	兼容性	理论最高速率	实际速率
802.11a	5GHz		54 Mb/s	22 Mb/s
802.11b	2.4GHz		11 Mb/s	5 Mb/s
802.11g	2.4GHz	兼容b	54 Mb/s	22 Mb/s
802.11n	2.4GHz/5GHz	兼容a/b/g	600 Mb/s	100 Mb/s
802.11ac W1	5GHz	兼容a/n	1.3 Gb/s	800 Mb/s
802.11ac W2	5GHz	兼容a/b/g/n	3.47 Gb/s	2.2 Gb/s
802.11ax	2.4GHz/5GHz		9.6Gb/s	

WiFi 6是第6代无线技术——IEEE 802.11 ax，其特点如下。

（1）速度

WiFi 6在160MHz信道宽度下，单流最高速率为1201Mb/s，理论最大数据吞吐量为9.6Gb/s。

（2）续航

这里的续航针对的是连接上WiFi 6路由器的终端。WiFi 6采用TWT（Target Wake Time，目标唤醒时间），路由器可以统一调度无线终端休眠和数据传输的时间，不仅可以唤醒、协调无线终端发送、接收数据的时机，减少多设备无序竞争信道的情况，还可以将无线终端分组到不同的TWT周期，增加睡眠时间，提高设备电池的寿命。

（3）延迟

WiFi 6平均延迟降低为20ms，WiFi 5平均延迟为30ms。当然，如果要使用WiFi 6，就需要使用包括支持WiFi6的路由器和终端。

6.2.2 无线局域网的安全技术

在无线局域网中，经常会使用以下技术来提高安全性。

1. 机密性保护

无线网络在实际应用过程中面临严重的信息泄露或被篡改的危险，数据泄露的威胁将严重影响无线网络的应用发展。因此，研究和解决机密性保护问题对无线网络的大规模应用具有重要意义。保证数据的机密性可以通过有线等效保密（Wired Equivalent Privacy，WEP）协议、临时密钥完整性协议（Temporal Key Integrity Protocol，TKIP）或VPN实现。WEP提供了机密性，

但是这种算法很容易被破解。而TKIP使用了更强的加密规则，可以提供更好的机密性。

2. 安全重编程

安全重编程指的是通过无线信道对整个网络进行代码镜像分发并完成代码安装，这是解决无线网络管理和维护的有效途径。因为无线网络通常布置在广阔并且环境恶劣的地方，攻击者可以利用重编程机制的漏洞发起一系列攻击。比如可以通过注入伪造的代码镜像获取整个网络的控制权。安全重编程技术主要解决无线网络中代码更新的验证问题，其目的在于防止恶意代码的传播和安装。因此，安全重编程一直是一个研究热点。

3. 用户认证

为了让具有合法身份的用户加入网络并获取其预订的服务，同时能够阻止非法用户获取网络数据，确保无线网络的外部安全，要求网络必须采用用户认证机制检验用户身份的合法性。用户认证是一种最重要的安全业务，在某种程度上所有其他安全业务均依赖于它。

对于无线网络的认证可以是基于设备的，通过共享的WEP密钥实现。也可以是基于用户的，使用可扩展身份验证协议（Extensible Authentication Protocol，EAP）实现。无线EAP认证可以通过多种方式实现，如EAP-TLS、EAP-TTLS、LEAP和PEAP。在无线网络中，设备认证和用户认证都应该实施，以确保最有效的网络安全性。用户认证信息应该通过安全隧道传输，从而保证用户认证信息交换是加密的。因此，对于所有的网络环境，如果设备支持，最好使用EAP-TTLS或PEAP。

4. 信任管理

作为对基于密码技术的安全手段的重要补充，信任管理在抵御无线网络中的内部攻击，鉴别恶意节点和自私节点，提高系统安全性、公平性、可靠性等方面有着显著的优势。以信任计算模型为核心的信任管理，尤其对于没有构建网络基础设施的自组织网络，提供了一种新的、有效的安全解决方案。

5. 安全的网络通信架构

网络通信架构包括网络接入协议及多种网络通信协议。无线网络应用领域的多样性决定了其构成的复杂性。建设安全的无线网络离不开安全的网络通信架构。

6.2.3 无线加密技术

在无线局域网中，常见的加密技术有WEP、WPA和WAPI等。

1. WEP

WEP使用64位或128位密钥，使用RC4对称加密算法对链路层数据进行加密，从而防止非授权用户的监听和非法用户的访问。有线等效保密协议加密时采用的密钥是静态的，各无线局域网终端接入网络时使用的密钥是一样的。有线等效保密协议具有认证功能，当WEP加密启用后，客户端要连接AP时，AP会发出一个Challenge Packet给客户端，客户端再利用共享密钥将此值加密后送回存取点，以进行认证对比，只有正确无误才能获准存取网络的资源。无线对等保密是802.11标准下定义的一种安全机制，设计用于保护无线局域网接入点和网卡之间通过空气

进行的传输。虽然WEP提供64位或128位密钥，但是仍然具有很多漏洞，因为用户共享密钥，只要有一个用户泄露密钥，就会对整个网络的安全性构成很大的威胁。而且WEP加密被发现有安全缺陷，可以在几分钟内被破解，因此现在的WEP已经不再是无线局域网加密的主流方式。

2. WPA 与 WPA2

WPA（WiFi Protected Access，WiFi保护性接入）是继承了WEP基本原理，而又克服了WEP缺点的一种新技术。WPA的核心是IEEE 802.1×和TKIP，它属于IEEE 802.11i的一个子集。WPA协议使用新的加密算法和用户认证机制，强化了生成密钥的算法，即使有不法分子对采集到的分组信息深入分析也无济于事，WPA协议在一定程度上解决了WEP破解容易的缺陷。

WPA2是WiFi联盟发布的第2代WPA标准。WPA2与后来发布的802.11i有类似的特性，它们最重要的共性是预验证，即在用户对延迟毫无察觉的情况下实现安全快速漫游，同时采用CCMP加密包代替TKIP，WPA2实现了完整的标准，但不能用在某些比较老的网卡上。

注意事项 WPA与WPA2的主要问题

WPA和WPA2都提供优良的安全能力，但也都有两个明显的问题。

- WPA或WPA2一定要启动，并且被选中用来代替WEP才有用，但是大部分的安装指引都把WEP列为第一选择。
- 在家中和小型办公室中选用“个人”模式时，为了安全的完整性，所用的密钥一定要比8个字符的密码长。

WPA加密方式目前有4种认证方式：WPA、WPA-PSK、WPA2和 WPA2-PSK。采用的加密算法有两种：AES和TKIP。

- **WPA**：WPA加强了生成加密密钥的算法，因此即便收集到分组信息并对其进行解析，也几乎无法计算出通用密钥。WPA中还增加了防止数据中途被篡改的功能和认证功能。
- **WPA-PSK**：WPA-PSK适用于个人或普通家庭网络，便用预先共享密钥，密钥设置的密码越长，安全性越高。WPA-PSK只能使用TKIP加密方式。
- **WPA2**：WPA2是WPA的增强型版本，与WPA相比，WPA2新增了支持AES的加密方式，取代了以往的RC4算法。
- **WPA2-PSK**：与WPA-PSK类似，适用于个人或普通家庭网络，使用预先共享密钥，支持TKIP和AES两种加密方式。

一般在家庭无线路由器设置页面上选择使用WPA-PSK或WPA2-PSK认证类型即可，对应设置的共享密码尽可能长，并且在使用一段时间后更换共享密码，确保家庭无线网络的安全。

3. WPA3

WPA3全名为WiFi Protected Access 3，是WiFi联盟组织于2018年1月8日在美国拉斯维加斯的国际消费电子展（CES）上发布的WiFi新加密协议，是WiFi身份验证标准WPA2技术的后续版本。

WPA3标准将加密公共WiFi网络上的所有数据，可以进一步保护不安全的WiFi网络。特别当用户使用酒店或旅游区WiFi热点等公共网络时，借助WPA3可创建更安全的连接，让黑客无法窥探用户的流量，难以获得私人信息。尽管如此，黑客仍然可以通过专门的、主动的攻击来窃取数据。但是，WPA3至少可以阻止强力攻击。

WPA3有以下4项新功能。

① 对使用弱密码的人采取“强有力的保护”。如果密码多次输错，将锁定攻击行为，屏蔽WiFi身份验证过程来防止暴力攻击。

② WPA3将简化显示接口受限，甚至包括不具备显示接口的设备的安全配置流程。能够使用附近的WiFi设备作为其他设备的配置面板，为物联网设备提供更好的安全性。用户能够使用自己的手机或平板电脑来配置另一个没有屏幕的设备（如智能锁、智能灯泡或门铃等小型物联网设备），设置密码和凭证，而不是任由其他人访问和控制。

③ 接入开放性网络时，通过个性化数据加密增强用户隐私的安全性，是对每个设备与路由器或接入点之间的连接进行加密的一个特征。

④ WPA3的密码算法提升至192位的CNSA等级算法，与之前的128位加密算法相比，增加了字典法暴力密码破解的难度。并使用新的握手重传方法取代WPA2的四次握手，WiFi联盟将其描述为“192位安全套件”。该套件与美国国家安全系统委员会国家商用安全算法（CNSA）套件相兼容，将进一步保护政府、国防和工业等更高安全要求的WiFi网络。

4. WAPI

无线局域网鉴别与保密基础结构（Wireless Authentication and Privacy Infrastructure，WAPI）于2003年在我国无线局域网国家标准GB 15629.11—2003中提出了针对有线等效保密协议安全问题的无线局域网安全处理方案。这个方案已经经过IEEE严格审核，并最终取得IEEE的认可，分配了用于WAPI协议的以太类型字段，这也是我国目前在该领域唯一获得批准的协议，同时也是我国无线局域网安全强制性标准。

与WiFi的单向加密认证不同，WAPI双向均认证，从而保证传输的安全性。WAPI安全系统采用公钥密码技术，鉴权服务器负责证书的颁发、验证与吊销等，无线客户端与无线接入点上都安装有AS（Access Server，访问服务器）颁发的公钥证书，作为自己的数字身份凭证。当无线客户端登录至无线接入点时，在访问网络之前必须通过AS对双方进行身份验证。根据验证的结果，持有合法证书的移动终端才能接入持有合法证书的无线接入点。

6.2.4 无线接入密码的破译与防范

无线接入密码是允许客户端连接无线接入点的凭证，关乎无线局域网的安全，现在主流的破译无线接入密码的方法就是暴力破解和钓鱼技术。

1. 暴力破解与防范

WEP这种加密方式属于明文密码，很容易可以读取到，所以已经被淘汰了。而WPA-PSK/WPA2-PSK加密方式传输的密码是经过加密的，只能通过暴力破解。暴力破解一般基于密码字典，通过运算后进行对比。

大部分的无线密码破解基于无线握手包的爆破，所谓握手包，是终端与无线设备（无线路由器）之间进行连接及验证所使用的数据包。所以黑客在使用工具侦听整个过程后，捕获到对方的数据，再通过暴力破解，计算出PSK，也就是密码。

破解的过程并不是单纯地使用密码去尝试连接。而是在本地对整个握手过程中需要的PSK进行运算。前提是终端在侦听过程中，与客户端进行连接，也就是有握手的过程，才能捕获握

手包。如果此时没有突发的连接，破解工具还可以强制连接的某终端断开连接，然后终端会重新连接，这样就能抓到数据包了。

将握手包抓取后在本地破解有很多优势。虽然现在路由器没有验证码。但是考虑到路由器策略，比如有些路由器可以设置拒绝这种高频连接。最重要的其实是效率问题，在本地进行模拟破解，只要硬件够强，每秒可以对比相当多的字典条目，这是在线破解远远不能比的。

暴力破解经常使用的工具是Aircrack -ng，一款用于破解无线802.11WEP及WPA-PSK加密的工具，是一个包含多款工具的无线攻击升级套装。

（1）启动网卡侦听模式

启动网卡的侦听模式后，可以对无线信号进行扫描，获取无线路由器的MAC地址、信道、验证方式等，如图6-5所示。

```
CH 14 ][ Elapsed: 36 s ][ 2021-06-18 11:29

BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

F8:8C:21:06:78:70  -40       17        1    0  11  540   WPA2 CCMP   PSK  FAST_310
78:02:F8:30:F0:53  -40       13        0    0  11  180   WPA2 CCMP   PSK  mytest
3C:F5:CC:1F:8E:45  -52       13        0    0   1  270   OPN              <length:  0>
AC:9E:17:A7:31:40  -59       12        5    0   4  195   WPA2 CCMP   PSK  lanxinhaibim
A8:E5:44:A7:AD:81  -59       15        0    0  11  130   WPA2 CCMP   PSK  <length:  0>
A8:E5:44:A7:AD:7D  -59       11        0    0  11  130   WPA2 CCMP   PSK  <length:  0>
A8:E5:44:A7:AD:7C  -59       15        2    0  11  130   WPA2 CCMP   PSK  BIM
3C:F5:CC:1F:8E:47  -63       13        1    0   1  270   WPA2 CCMP   PSK  qvit-wireless
E8:A1:F8:45:7A:28  -64       10        0    0   4  130   WPA2 CCMP   PSK  ChinaNet-UYaY
74:B7:B3:41:D2:B4  -63       14        0    0   2  130   WPA2 CCMP   PSK  ChinaNet-zxdA
D8:38:0D:4B:EB:61  -62       20        9    0   3  270   WPA2 CCMP   PSK  qvkj257
B8:DD:71:28:DE:E7  -66        2        0    0   4  360   WPA2 CCMP   PSK  yunxuntong1
0C:83:9A:27:EE:75  -66        2        0    0   6  360   WPA2 CCMP   PSK  <length:  0>
DC:71:37:D8:67:28  -66        9        0    0   9  130   WPA2 CCMP   PSK  ChinaNet-LVLb
```

图 6-5

（2）抓取握手包

通过命令让网卡侦听，并重新连接的设备的连接验证中抓取握手包，存储在本地，如图6-6所示。

```
└─# airodump-ng -c 11 --bssid 78:02:F8:30:F0:53 -w /home wlan0
13:38:02  Created capture file "/home-01.cap".

 CH 11 ][ Elapsed: 4 mins ][ 2021-06-18 13:42 ][ WPA handshake: 78:02:F8:30:F0:53

 BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

 78:02:F8:30:F0:53  -34  43     1254      219    1  11  180   WPA2 CCMP   PSK  mytest

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

 78:02:F8:30:F0:53  98:FA:E3:F0:5A:B9  -32    1e- 6    296      221  EAPOL  mytest
Quitting ...
```

图 6-6

知识点拨

强制获取握手包

如果此时没有新加入设备，可以通过命令查看该路由器接入的设备，如图6-7所示，并可以主动断开某设备，让其重新连接，从而获取到握手包。使用该功能也可以让某些无线终端无法正常联网。

```
└─# airodump-ng -c 11 --bssid 78:02:F8:30:F0:53 -w /home wlan0
13:38:02  Created capture file "/home-01.cap".

 CH 11 ][ Elapsed: 4 mins ][ 2021-06-18 13:42 ][ WPA handshake: 78:02:F8:30:F0:53

 BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

 78:02:F8:30:F0:53  -34  43     1254      219    1  11  180   WPA2 CCMP   PSK  mytest

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

 78:02:F8:30:F0:53  98:FA:E3:F0:5A:B9  -32    1e- 6    296      221  EAPOL  mytest
Quitting ...
```

图 6-7

（3）暴力破解

握手包被抓取并保存到本地后，就可以使用暴力破解工具和有效字典的组合来破解密码了。因为没有验证码，也不存在在线破解的响应问题，所以破解效率极高。如果密码字典正好有该密码，则会显示出来，如图6-8所示。

```
                          Aircrack-ng 1.6

 [00:00:00] 4/8 keys tested (43.33 k/s)

 Time left: 0 seconds                                      50.00%

                        KEY FOUND! [ 87654321 ]


 Master Key     : E4 7B 98 1C EF 3F 80 D6 08 25 0D 0F CA 63 15 21
                  5D 1B 31 1D A8 08 C0 61 30 EA C3 91 72 BE 5F E8

 Transient Key  : 85 65 48 4A A1 B5 E8 8E D2 1D 5C D1 AC EF 08 1F
                  EE FC 47 56 3E 29 5B B9 D8 D9 9F E6 12 37 10 03
                  27 69 BD FF 87 7E 5F 18 47 60 00 00 00 00 00 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

 EAPOL HMAC     : E5 10 2B 54 26 BD 81 4A C0 0E 54 D1 CC E9 07 15
```

图 6-8

理论上来说，只要有足够的时间，就可以通过对比握手包，破译出无线密码。所以在防范中，要为无线路由器设置复杂的连接密码，并采用最新的WAP3防范。

2. 伪装钓鱼及其防范

伪装钓鱼方式并不属于破解范畴，而是和钓鱼网站一样，诱导用户自己填写明文密码，从而被黑客掌握。常使用的软件是Fluxion，其原理及过程如下。

① 扫描WiFi信号。

② 抓取握手包。

③ 使用Web接口模拟正常的接入点，即模拟一个假的AP，如图6-9所示。

④ 生成一个MDK3进程。如果普通用户已经连接到这个WiFi，也会被提示输入WiFi密码。

⑤ 随后启动一个模拟的DNS服务器，并且抓取所有的DNS请求，把请求重新定向到一个含有恶意脚本的HOST地址，如图6-10所示。

图 6-9

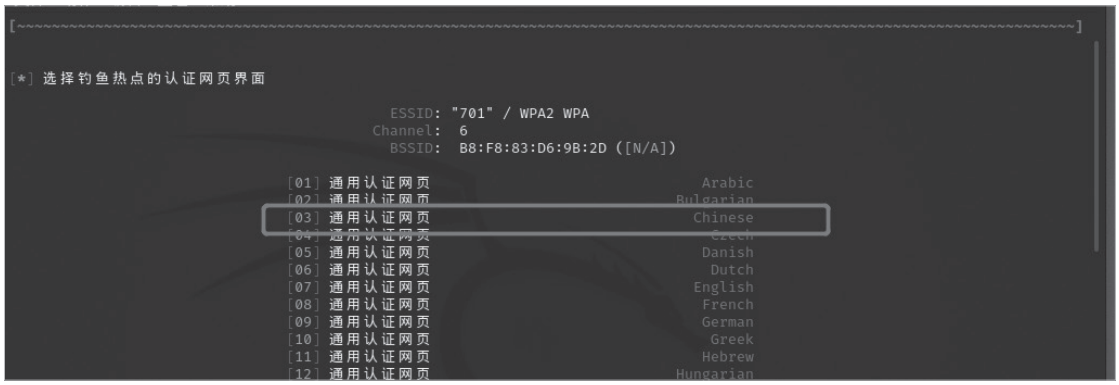


图 6-10

⑥ 随后会弹出一个窗口，提示用户输入正确的WiFi密码。

⑦ 用户输入的密码将和第二步抓到的握手包做比较，以核实密码是否正确。

当用户输入正确的密码时，Fluxion会自动结束程序、显示密码，并生成破解日志。程序结束后制作的虚假AP自然就不见了，这时提交了真实密码的机器会自动连上真实的AP，作为不知情的用户来说，可能只是感觉信号不太好。

对于伪装钓鱼，用户只要了解正常的连接无线的步骤，并坚持不在非正常位置输入各种密码，就可以避免大部分网络钓鱼的威胁。

6.2.5 无线局域网安全防御措施

提高无线网络安全的方法有多种，针对不同的情况采用不同的方法，也可以多种方法相结合。

1. 使用高级的无线加密协议

不要使用WEP，大多数没有经验的黑客也能够迅速和轻松地突破WEP加密。若使用WEP，则要升级到具有802.1×身份识别功能的802.11i的WPA2协议，有条件的用户也可以使用更高级的WPA3协议。

2. 禁止非授权的用户联网

无线网络和有线网络虽然都是计算机网络，但有很大的区别。无线网络是放射状的，不存

在专有线路连接，比有线网络更容易识别和连接。因此，保证保障无线网络的安全比有线网络更加困难。保证无线连接安全的关键是禁止非授权用户访问无线网络，即安全的接入点对非授权用户是关闭的，非授权用户无法接入网络。

3. 禁用 DHCP 协议

动态主机配置协议（DHCP）在很多网络中被普遍使用，给网络管理提供了便利条件，但同时给网络带来了安全风险，因此应该禁用动态主机配置协议。采用这个策略后，即使黑客能使用无线接入点，但不知道IP地址等信息，会增加黑客破解无线网络的难度，这样可以提高无线网络的安全性。

4. 使用访问列表

为了更好地保护无线网络，可以设置一个访问列表，使无线路由器只允许在规则内的MAC地址的设备进行通信，或者禁止黑名单中的MAC地址访问，如图6-11所示。启用MAC地址过滤，无线路由器会拦截禁止访问的设备所发送的数据包，将这些数据包丢弃。因此，对于恶意攻击的主机，即使变换IP地址也无法进行访问。但这项功能并不是所有无线接入点都支持，并且需要统计并输入需要过滤的MAC地址。

图 6-11

5. 禁止 SSID 广播

无线接入点的服务集标识符（SSID）是无线接入的身份标识，是无线网络用于无线服务连接的一项功能，用户通过它连接到无线网络。默认情况下任何在此设备覆盖范围内的无线访问设备都可以获得SSID信息。可以禁止SSID广播，隐藏该网络名，如图6-12所示。只有知道SSID的用户才能进行连接，这在一定程度上起到了安全防范的作用。

图 6-12

6. 修改管理账户名和密码

有很多用户在使用无线网络时自己修改了相关的安全设置，但是忽略了管理账户和密码的修改，这给网络安全带来了隐患。因此，在对无线网络进行安全设置时，要先对管理账号和密码进行修改。

7. 修改接入点 IP 地址

大部分路由器的管理IP为192.168.1.1或192.168.0.1，这样的接入IP如果不进行修改，很容易被攻击者利用，通过嗅探和扫描找到网络的漏洞。因此，在设置无线网络安全时，可以将这个IP地址修改为其他值，如192.168.50.1，结合前面禁用DHCP的功能，使黑客的攻击难度大幅增加。

6.3 网站安全与入侵检测

因特网之所以成为最大的广域网，除了TCP/IP协议外，还有其中大量的共享资源，而承载这些资源的就是大大小小的各种网站，所以网站的安全对于因特网非常重要。下面介绍网站安全的相关知识。

6.3.1 网站概述

网站（Web Site）是指在因特网上，根据一定的规则，使用HTML（标准通用标记语言）等工具制作的、用于展示特定内容的相关网页的集合。简单地说，网站是一种沟通工具，人们可以通过网站发布自己想要公开的资讯，或者利用网站提供相关的网络服务。人们可以通过网页浏览器访问网站，获取自己需要的资讯，或者享受其他网络服务。网站按照不同的标准也分成不同的类别。

- 按照编程语言，分为ASP网站、PHP网站、JSP网站、ASP.NET网站等。
- 按照客户端，分为计算机访问的常规网站和手机查看的H5网站。
- 按照网站产生方式，分为静态网站和使用脚本语言的动态网站。

6.3.2 网站常见攻击方式及防范

黑客攻击网站，通常使用以下的技术手段。

1. 流量攻击

流量攻击即拒绝服务攻击，包括SYN泛洪攻击、Smurf攻击以及DDoS攻击。因为在服务器看来都是正常的访问，所以最不容易做防御策略。理论上除非带宽够大，否则所有网站都是可以被攻击的。当然，服务器可以在被攻击时关闭服务、拒绝服务。但黑客的目的就是让其他正常用户的访问受阻或受限。

对于正常的用户来说，这种攻击会使网页无法正常打开，而在网站看来，会发生网站程序停止服务，无法抓取网站，清空索引和排名，流量下滑等。

防御手段，除了选择有大型安全防火墙的主机服务商（如阿里云）外，还需要网站有监控系统、CDN防护以及服务器自身的安全防护等（安全狗）。

2. 域名攻击

域名攻击包括域名所有权和域名注册商被恶意转移、DNS域名劫持等，阻止域名解析或者解析到黑客设置的服务器或钓鱼网站中，从而获利。

所以要选择大型知名的域名注册商，填写真实信息并锁定域名，禁止转移。保证域名注册手机、邮箱的安全。定时查询域名的状态，如图6-13所示。

图 6-13

3. 恶意扫描

前面介绍扫描端口和漏洞时，以本地主机和网站为目标。如果使用其他互联网网站，就属于恶意扫描了。通过扫描发现开放的端口和漏洞，从而入侵网站系统。

针对恶意扫描，要做到除了必需的端口，尽量关闭或更改常用的监听端口，并选择有专业防火墙的主机厂商，在网站主机中安装安全狗等。

4. 网页篡改

网页篡改指针对网站程序漏洞，植入木马（Webshell，跨站点脚本攻击），篡改网页，添加黑链或嵌入非网站信息，甚至创建大量网页。现在很多网站会对所收录的网站进行定期的安全检测，如果出现某网站存在网页篡改，会有恶意代码和链接等，则会在搜索结果中提示安全风险，或阻止网页跳转访问。

这种情况就需要下载更新补丁，修补漏洞，经常备份，经常使用第三方的检测平台进行检测，如图6-14所示。

图 6-14

5. 数据库攻击

SQL注入攻击是最普遍的安全隐患之一，它利用应用程序对用户输入数据的信任，将恶意SQL代码注入应用程序中，用来执行攻击者的操作。这种攻击可以导致敏感信息泄露、数据损坏或删除以及系统瘫痪，给企业和个人带来巨大损失。

数据库被入侵后，会造成用户信息泄露、数据表被篡改、植入后门等，数据库被篡改比网页文件被篡改危害大得多，因为现在基本上都是动态网站，而这些网页都是通过数据库生成的。

防范措施除了选择带有强大防火墙的主机厂商外，还要配备数据库防火墙，以及在表单提交处设置验证。

6.3.3 入侵检测技术

入侵检测技术是预防和判断网站或主机被入侵的一种检测手段。

1. 入侵检测系统简介

入侵检测系统（Intrusion Detection System，IDS）是一种对网络传输进行即时监视，在发现可疑传输时发出警报或者采取主动应急措施的网络安全设备。与其他网络安全设备的不同之处在于，IDS是一种积极主动的安全防护技术。IDS最早出现在1980年4月。20世纪80年代中期，IDS逐渐发展成为入侵检测专家系统（IDES）。1990年，IDS分化为基于网络的IDS和基于主机的IDS，后来又出现分布式IDS。目前IDS发展迅速，已有人宣称IDS可以完全取代防火墙。

根据信息来源不同，IDS可分为基于主机的IDS和基于网络的IDS，根据检测方法不同，IDS又可分为异常入侵检测和误用入侵检测。不同于防火墙，IDS是一个监听设备，对IDS的部署，唯一的要求是：IDS应当挂接在所有关注流量都必须流经的链路上。IDS在交换式网络中的位置一般选择在尽可能靠近攻击源或者尽可能靠近受保护资源的位置。

2. 入侵检测系统的组成

入侵检测系统通常被分为四个组件：

- **事件产生器（event generators）**：目的是从整个计算环境中获得事件，并向系统的其他部分提供此事件。
- **事件分析器（event analyzers）**：经过分析得到的数据，产生分析结果。
- **响应单元（response units）**：对分析结果做出反应的功能单元，可以做出切断连接、改变文件属性等强烈反应，也可以只是简单的报警。
- **事件数据库（event databases）**：存放各种中间数据和最终数据的地方的统称，可以是复杂的数据库，也可以是简单的文本文件。

3. 入侵检测软件

Easyspy是一款网络入侵检测和流量实时监控软件。支持Cut-Off动作。通过Cut-Off动作和“数据包事件”，可以实现常见的防火墙功能，比如对端口或IP地址的封堵，通过灵活的事件规则，可以封堵P2P应用，比如eMule、eDonkey、Bittorrent，当然还可以封堵其他任何应用。

作为一个入侵检测系统，可以用来快速发现并定位诸如ARP攻击、DoS/DDoS、分片IP报文攻击等恶意攻击行为，帮助发现潜在的安全隐患。Easyspy又是一款Sniffer软件，可以用来进行

故障诊断，快速排查网络故障，准确定位故障点，评估网络性能，查找网络瓶颈从而保障网络质量。采用嗅探优先的协议识别方式。这样就解决了一些协议采用知名端口躲避识别的问题。

下载、安装并运行，在主界面中可以通过图形界面监控当前的网络利用率、包的大小分布、当前连接的状态以及通信最多的几台主机。物理层、网络层、传输层和应用层的状态如图6-15所示。和其他抓包软件类似，用户可以查看当前各种实时的统计信息。

图 6-15

6.3.4 网站抗压检测

很多时候会使用第三方软件或网站进行网站的抗压性测试，来查看网站是否有漏洞，抵御进攻的能力怎样。

1. 网站测试内容

在网站制作好或者上线后，需要进行测试。网站测试主要包括以下内容。

- **UI测试**：也就是测试网站页面的美观度和合理度等。
- **链接测试**：查看链接是否正常，会不会报错等。
- **表单测试**：各种表单是否满足要求，会不会冲突，采集的数据能不能正常存储等。
- **兼容性测试**：不同平台、不同系统是不是都能正常访问等。
- **网络配置测试**：查看网速，查看不同运营商网络是否都能访问等。
- **负载测试**：查看多个用户同时访问，能不能正常提供服务等。
- **压力测试**：查看几百、几千、几万人同时访问时网站是否能正常应对等。
- **安全测试**：查看各种安全信息以及脚本语言是否有漏洞等。
- **接口测试**：查看接口是否有问题等。

2. 使用网站测试

现在除了工具以外，还可以使用第三方网站进行在线压力测试。这些网站可以提供正常的压力测试，如模拟1000人次请求，并发数100，如图6-16所示。

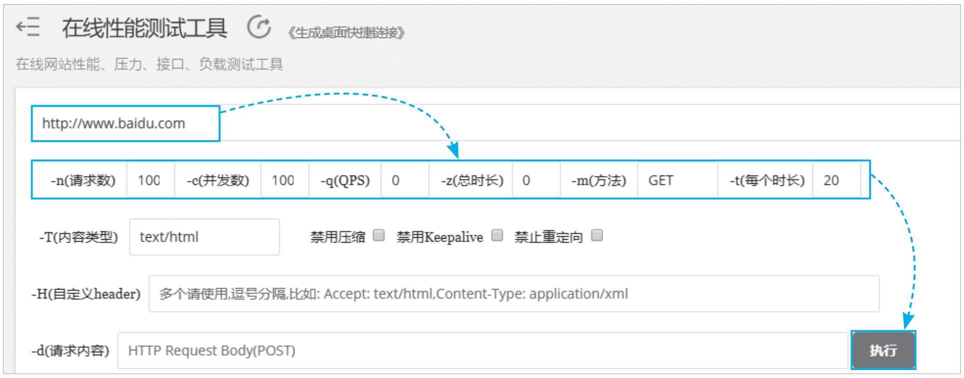
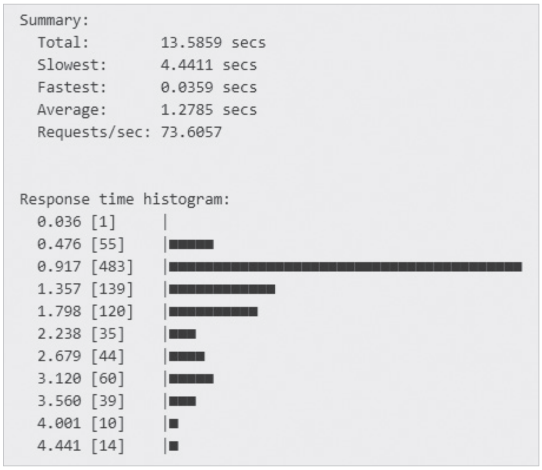


图 6-16

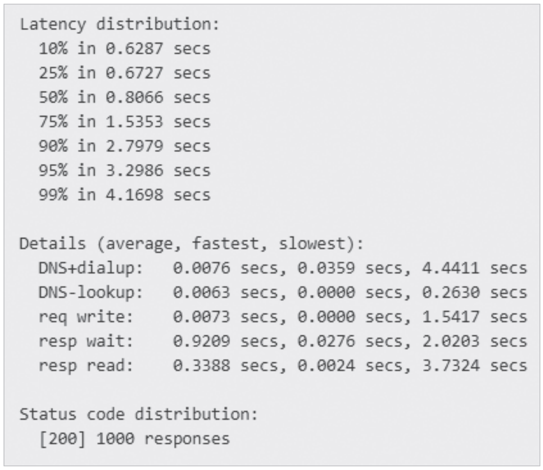
得到结果后进行分析，如图6-17和图6-18所示。



```
Summary:
  Total:        13.5859 secs
  Slowest:      4.4411 secs
  Fastest:      0.0359 secs
  Average:      1.2785 secs
  Requests/sec: 73.6057


Response time histogram:
  0.036 [1]     |
  0.476 [55]    |■■■■■
  0.917 [483]   |■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■
  1.357 [139]   |■■■■■■■■■■■■
  1.798 [120]   |■■■■■■■■■■
  2.238 [35]    |■■■
  2.679 [44]    |■■■■
  3.120 [60]    |■■■■■
  3.560 [39]    |■■■
  4.001 [10]    |■
  4.441 [14]    |■
```

图 6-17



```
Latency distribution:
  10% in 0.6287 secs
  25% in 0.6727 secs
  50% in 0.8066 secs
  75% in 1.5353 secs
  90% in 2.7979 secs
  95% in 3.2986 secs
  99% in 4.1698 secs

Details (average, fastest, slowest):
  DNS+dialup:  0.0076 secs, 0.0359 secs, 4.4411 secs
  DNS-lookup:  0.0063 secs, 0.0000 secs, 0.2630 secs
  req write:   0.0073 secs, 0.0000 secs, 1.5417 secs
  resp wait:   0.9209 secs, 0.0276 secs, 2.0203 secs
  resp read:   0.3388 secs, 0.0024 secs, 3.7324 secs

Status code distribution:
  [200] 1000 responses
```

图 6-18

知识点拨

端口扫描

除了测试网站连接性能，还可以进行端口扫描，如图6-19所示。

图 6-19

3. 使用软件测试

如使用DirBuster软件进行网站目录扫描，如图6-20所示。DirBuster软件支持全部的Web目录扫描方式，既支持网页爬虫方式扫描，也支持基于字典的暴力扫描，还支持纯暴力扫描。该软件使用Java语言编写，提供命令行（Headless）和图形界面（GUI）两种模式。其中，图形界面模式功能更为强大。用户不仅可以指定纯暴力扫描的字符规则，还可以设置以URL模糊方式构建网页路径。同时，用户还可对网页解析方式进行各种定制，提高网址解析效率。

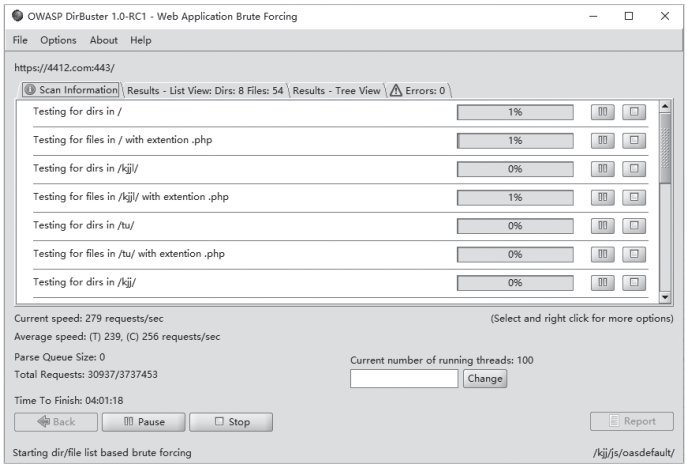


图 6-20

除了网站目录扫描外，还可以对网站进行DDoS压力测试，常见的LOIC如图6-21所示。LOIC是一款专著于Web应用程序的DoS/DDoS攻击工具，它可以用TCP数据包、UDP数据包、HTTP请求对目标网站进行DDoS/DoS测试。

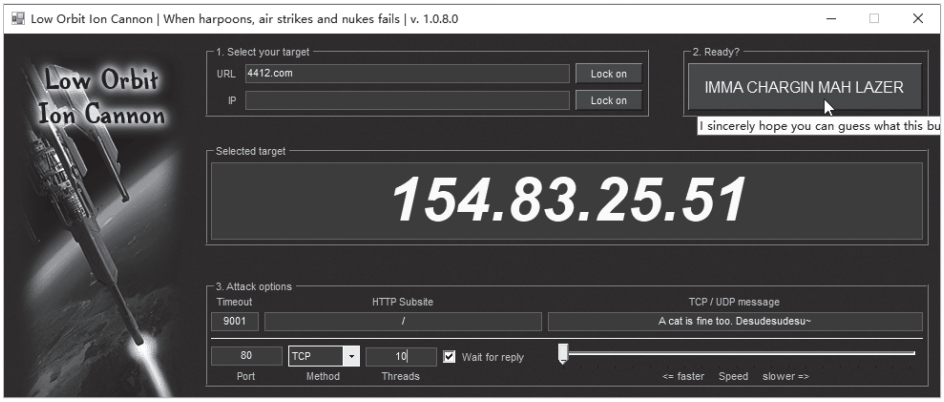


图 6-21

知识延伸：无线摄像头的安全防范

随着家庭安防需求的提高，摄像头已经进入了千家万户。而无线摄像头的安全也日趋严峻，很多黑客专门入侵摄像头，通过录像进行勒索。

1. 修改远程默认查看密码

很多摄像头使用默认的管理员账户和密码，这本身就存在非常大的安全隐患，所以必须修改

默认的查看密码，如图6-22所示。

图 6-22

2. 修改远程查看的端口号

除了修改密码外，还要修改远程查看的端口号，以防止暴力破解，如图6-23所示。

图 6-23

3. 其他注意事项

除了以上两点外，还可以设置摄像头的启动时间，在家里有人的情况下，关闭、遮盖摄像头，或者将摄像头调到没有人的角度，以便保护个人隐私。